COPYRIGHT

Copyright ©2007/2008 by this company. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written permission of this company.

This company makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not this company, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Further, this company reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

All brand and product names mentioned in this manual are trademarks and/or registered trademarks of their respective holders.

Federal Communication Commission
Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio technician for help.

FCC Caution

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the authority to operate equipment.

The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Federal Communications Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20cm (8 inches) during normal operation.

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/EC OF THE EUROPEAN PARLIAMENT AND THE COUNCIL of March 9, 1999 on radio equipment and telecommunication terminal Equipment and the mutual recognition of their conformity (R&TTE)
The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8, 2000.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

EU Countries Intended for Use

The ETSI version of this device is intended for home and office use in Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, the Netherlands, Portugal, Spain, Sweden, and the United Kingdom.
The ETSI version of this device is also authorized for use in EFTA member states: Iceland, Liechtenstein, Norway, and Switzerland.

EU Countries Not intended for use

None.

CONTENTS

1 INTRODUCTION 1

1.1 Features.....1
1.2 Specifications.....1
1.3 Package Contents.....2

2 INSTALLATION PROCEDURE 3

3 SETUP WIZARD.....10

4 CONFIGURATION UTILITY 14

3.1 Utility Overview.....15
3.2 Available Network.....17
3.3 General.....18
3.4 Profile.....20

3.4.1 Configure the Profile.....21

3.5 Advanced.....25
3.6 Status.....28
3.7 Statistics.....29
3.8 Wi-Fi Protected Setup.....30
3.9 Software AP.....31

3.8.1 AP Properties Setting.....32

3.8.2 AP Advanced.....33

3.8.3 AP Statistics.....34

3.8.4 ICS.....35

5 TROUBLESHOOTING.....36

1 Introduction

Thank you for purchasing EMTEC 802.11g Wireless LAN USB Adapter. This adapter complies with IEEE 802.11g standard, which supports up to 54Mbps high-speed wireless network connections. It can also work with IEEE 802.11b devices. When the adapter connects to 11b devices, the link speed will be up to 11Mbps.

For WLAN security issues, this adapter supports 64/128-bit WEP data encryption that protects your wireless network from eavesdropping. It also supports WPA (Wi-Fi Protected Access) feature technology. Client users are required to authorize before accessing to APs or AP Routers, and the data transmitted in the network is encrypted/decrypted by a dynamically changed secret key. Furthermore, this adapter supports WPA2 function, WPA2 provides a stronger encryption mechanism through AES (Advanced Encryption Standard), which is a requirement for some corporate and government users.

The power consumption of the adapter is also very low. Furthermore, this adapter provides several levels of power saving modes allowing user customizes the way of saving the power from his/her portable or handheld devices.

This adapter is cost-effective, together with the versatile features; it is the best solution for you to build your wireless network.

1.1 Features

- Works with both IEEE 802.11b and IEEE 802.11g products.
- High-speed transfer data rate - up to 54Mbps.
- High throughput supports multi-media data bandwidth requirement.
- Supports 64/128-bit WEP Data Encryption, WPA/WPA2 (TKIP with IEEE 802.1x) and AES.
- Automatic fallback increases data security and reliability.
- Supports the most popular operating system: Windows 98SE/Me/2000/XP/Vista.
- Supports USB 2.0 interface.

1.2 Specifications

- Standard: IEEE 802.11b/g
- Interface: USB 2.0 Type A
- Frequency Band: 2.4000 ~ 2.4835GHz (Industrial Scientific Medical Band)
- Modulation: OFDM with BPSK, QPSK, 16QAM, 64QAM (11g)

  BPSK, QPSK, CCK (11b)
- Data Rate: 54/48/36/24/18/12/11/9/6/5.5/2/1Mbps auto fallback
- Security: 64/128-bit WEP Data Encryption, WPA/WPA2 (TKIP with IEEE 802.1x) and AES

- Antenna: Printed Antenna
- Drivers: Windows 98SE/Me/2000/XP/Vista
- LEDs: Link/Activity
- Transmit Power: 11g: 14±1dBm, 11b: 17±1dBm
- Dimension: 9(H) x 27(W) x 87(D) mm
- Temperature: 32~131°F (0 ~55°C)
- Humidity: Max. 95% (NonCondensing)
- Certification: FCC, CE

1.3 Package Contents

Before you begin the installation, please check the items of your package. The package should include the following items:

- One USB Adapter
- One CD (Driver/Utility/User's Manual)
- One User Manual

If any of the above items is missing, contact your supplier as soon as possible.

2 Installation Procedure

Before you proceed with the installation, please notice following descriptions.

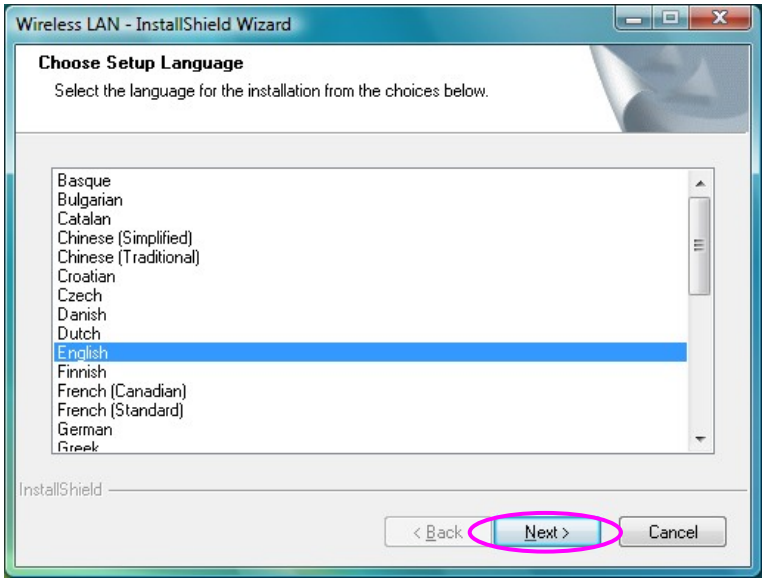
Note 1: The following installation was operated under Windows Vista. (Procedures are similar for Windows 98SE/Me/2000/XP.)

Note 2: If you have installed the Wireless Adapter driver & utility before, please uninstall the old version first.

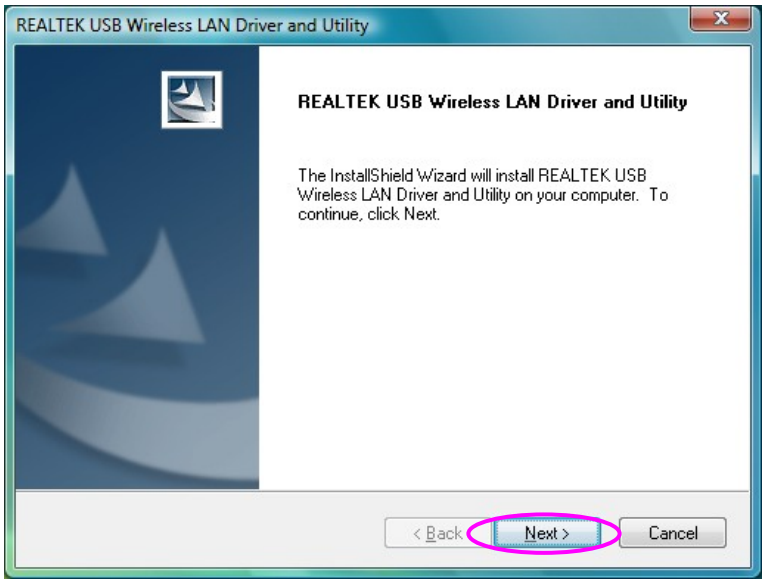
I. Install the Driver and Utility

A. Insert the Installation CD to your CD-ROM Drive. Execute the “Setup.exe” program.

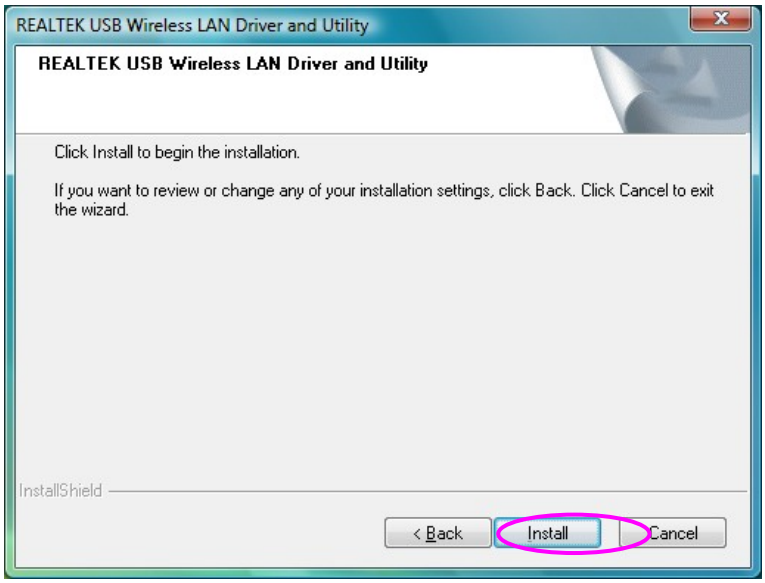
B. Select the Setup Language and click “Next” to proceed.



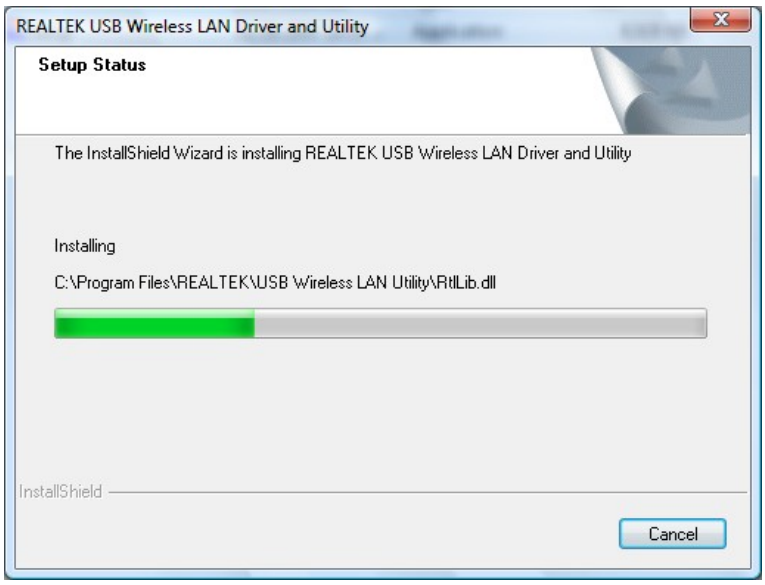
C. Click “Next” to start installing driver and utility.

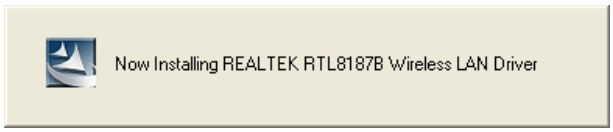

REALTEK USB Wireless LAN Driver and Utility
REALTEK USB Wireless LAN Driver and Utility
The InstallShield Wizard will install REALTEK USB Wireless LAN Driver and Utility on your computer. To continue, click Next.
< Back
Next >
Cancel

D. Click “Install” to start the installation.

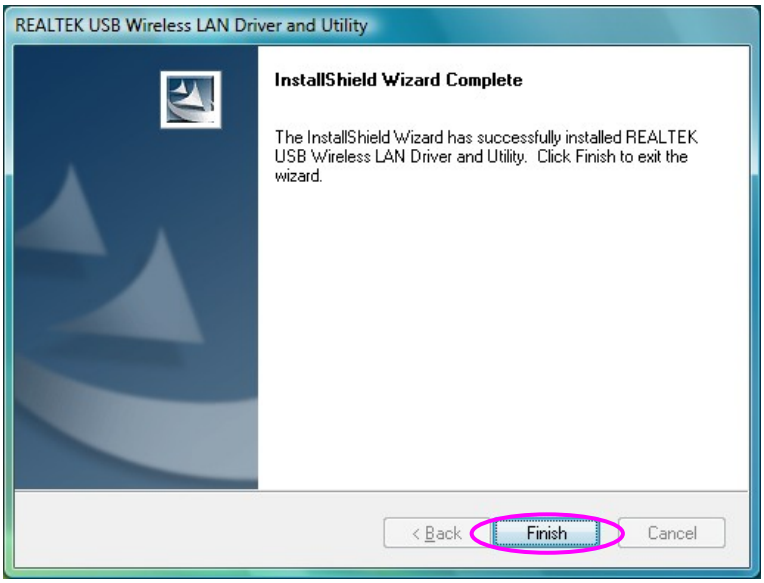

REALTEK USB Wireless LAN Driver and Utility
REALTEK USB Wireless LAN Driver and Utility
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
InstallShield
< Back
Install
Cancel

E. The system starts to install the driver and utility.


REALTEK USB Wireless LAN Driver and Utility
Setup Status
The InstallShield Wizard is installing REALTEK USB Wireless LAN Driver and Utility
Installing
C:\Program Files\REALTEK\USB Wireless LAN Utility\RtlLib.dll
InstallShield
Cancel



F. Click “Finish” to complete the software installation.


REALTEK USB Wireless LAN Driver and Utility
InstallShield Wizard Complete
The InstallShield Wizard has successfully installed REALTEK USB Wireless LAN Driver and Utility. Click Finish to exit the wizard.
< Back
Finish
Cancel

G. Please plug the USB adapter into the USB port of the computer.

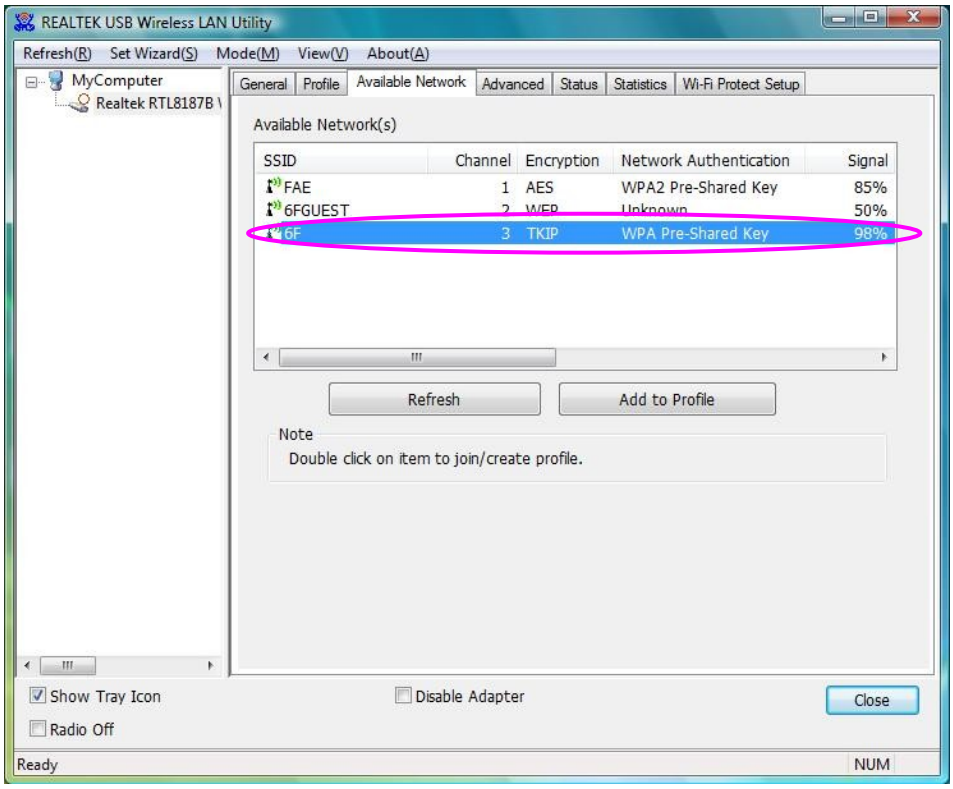
H. The system will auto detect the USB adapter and complete the drivers installation for the adapter automatically.

I. You are now able to use the USB adapter.

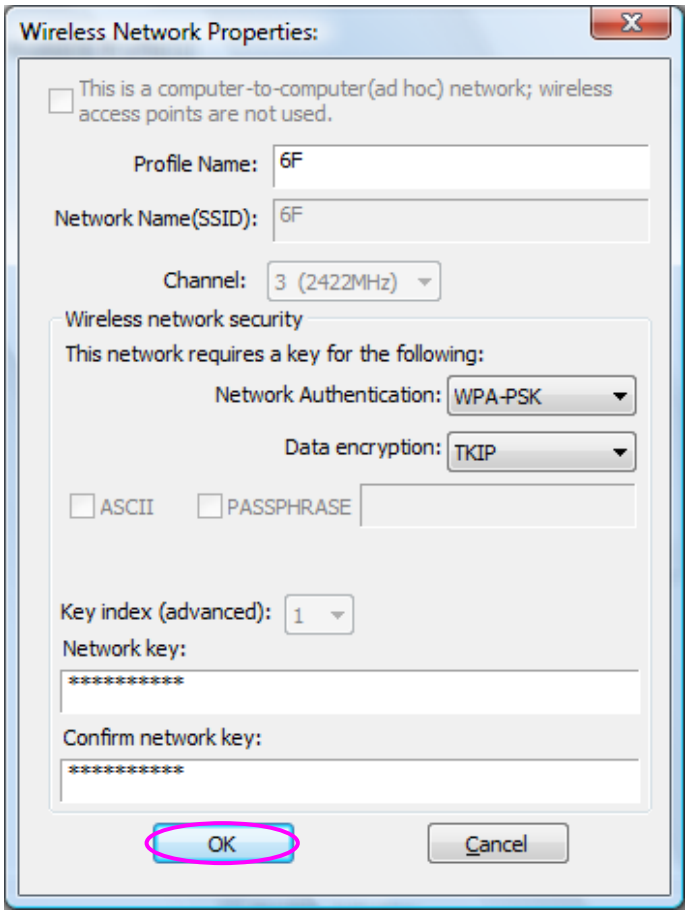
II. Connect to Wireless Access Point

A. To start configuring the adapter, double click the icon in the system tray.

B. The utility of the adapter is displayed. Click “Available Network” and double-click on the wireless access point you want to connect to.



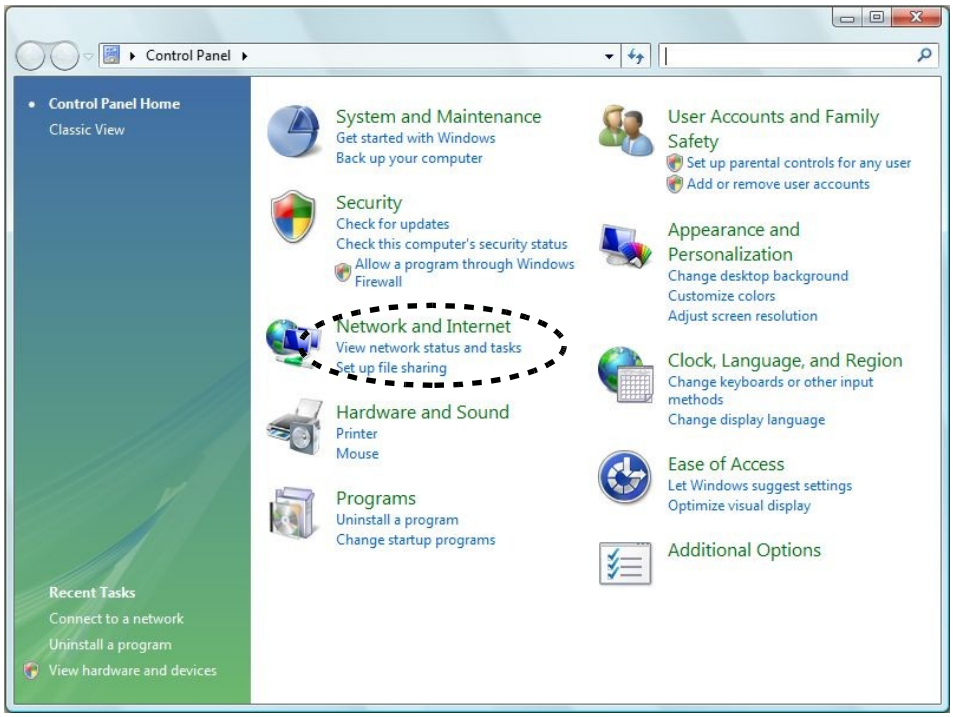
C. Input the security setting if the Access Point has enabled the security and click “OK” to start network connection.



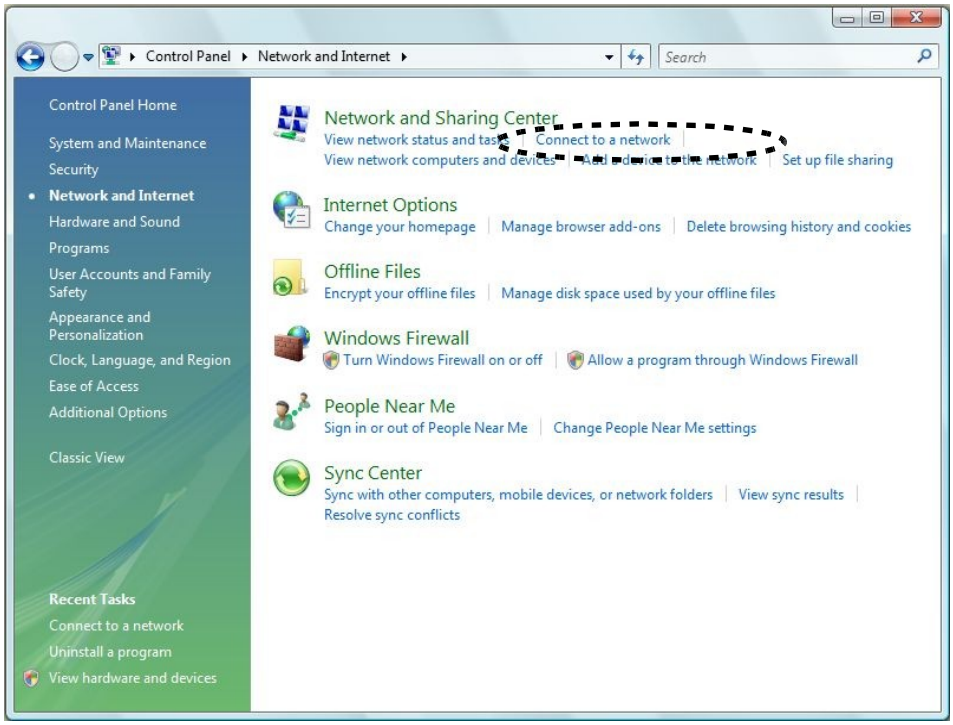
**** Use Windows Zero Configuration on Windows Vista:***

For Windows Vista user, you can use Windows Zero Configuration to connect to wireless access point.

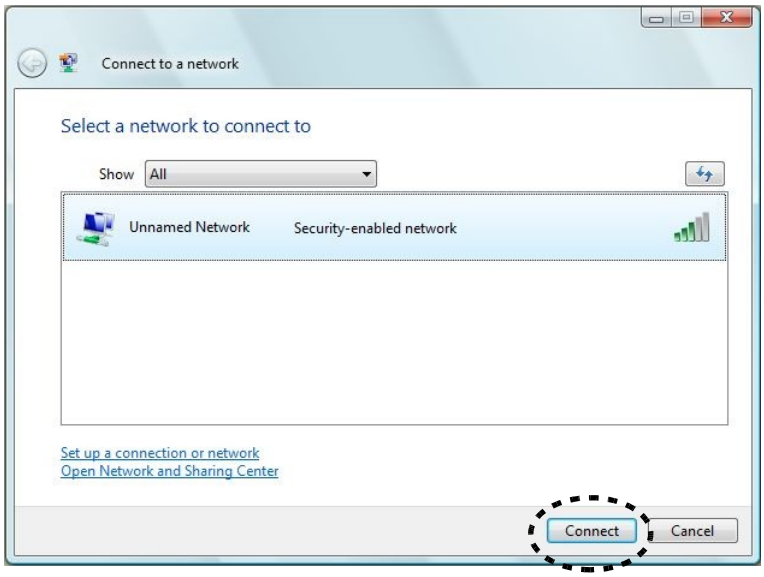
A. Click ‘Start’ button, then click ‘Control Panel. Click ‘Network and Internet’ in Control Panel.



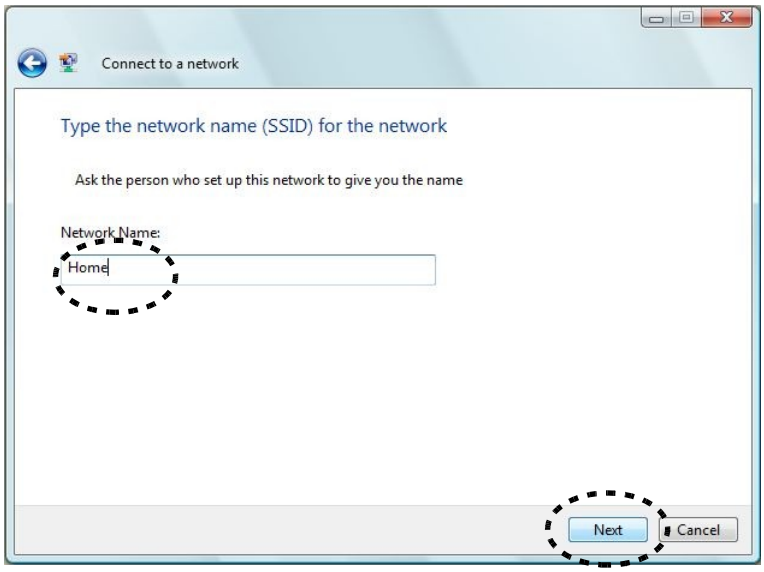
B. Click ‘Connect to a network’ under ‘Network and Sharing Center’.



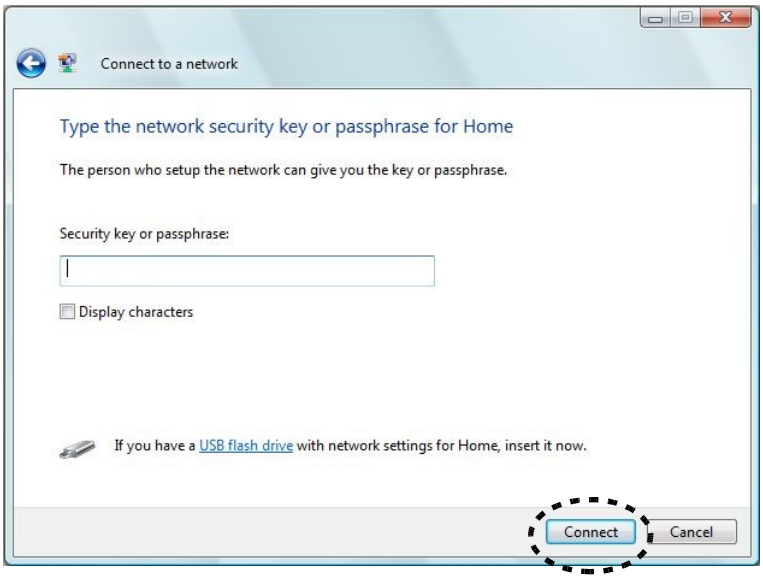
C. Click the access point you want to use if it's shown, then click 'Connect'.



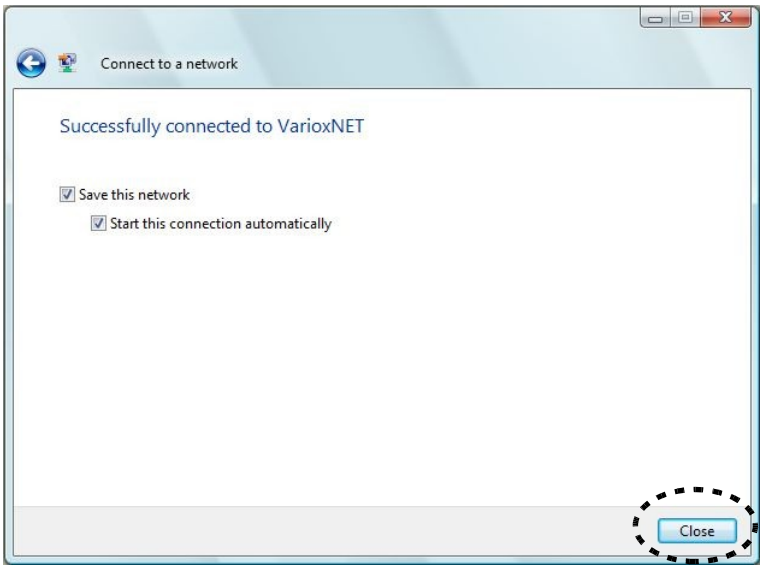
D. If it's an unnamed access point (i.e. the SSID of this wireless access point is hidden), you'll be prompted input it's name, and the name must be identical to the SSID setting of the wireless access point you're connecting to. Click 'Next'.


Connect to a network
Type the network name (SSID) for the network
Ask the person who set up this network to give you the name
Network Name:
Home
Next
Cancel

E. If the access point is protected by encryption method, you have to input its security or passphrase here. It must match the encryption setting on the access point. Click ‘Connect’.


Connect to a network
Type the network security key or passphrase for Home
The person who setup the network can give you the key or passphrase.
Security key or passphrase:
Display characters
If you have a USB flash drive with network settings for Home, insert it now.
Connect
Cancel

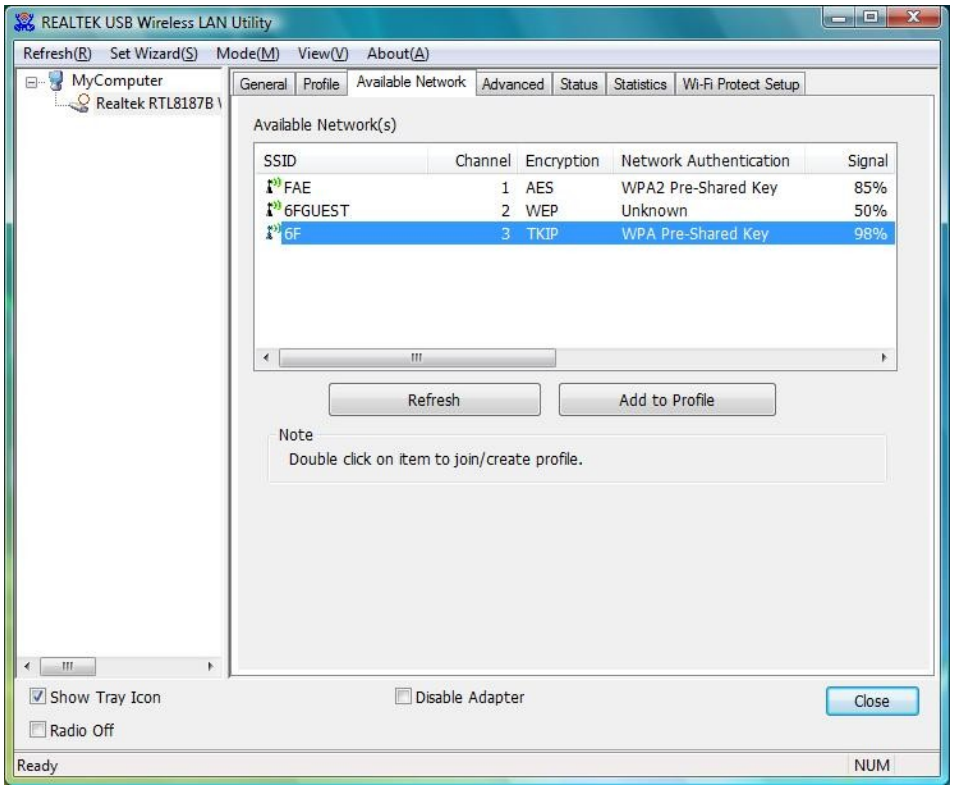
F. If you can see this image, the connection between your computer and wireless access point is successfully established. Click ‘Close’ to start network connection.



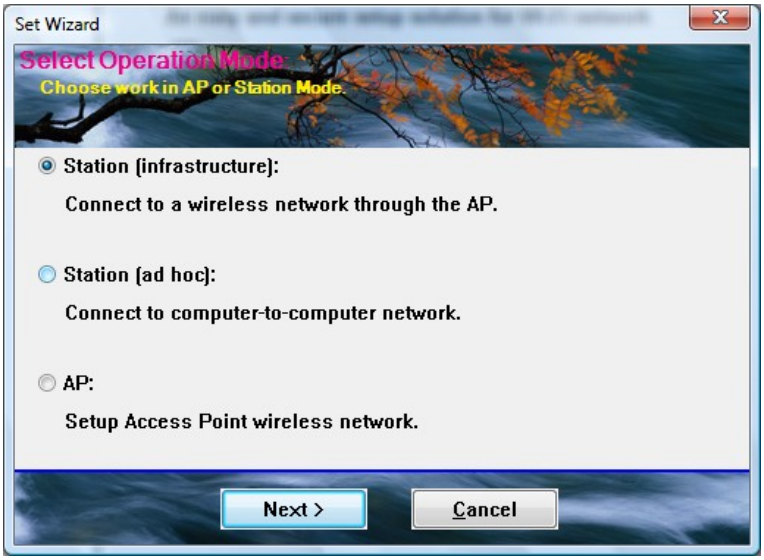
3 Setup Wizard

The utility supports a quick setup wizard for you to connect to the wireless network simply. Please follow the step below to run the setup wizard.

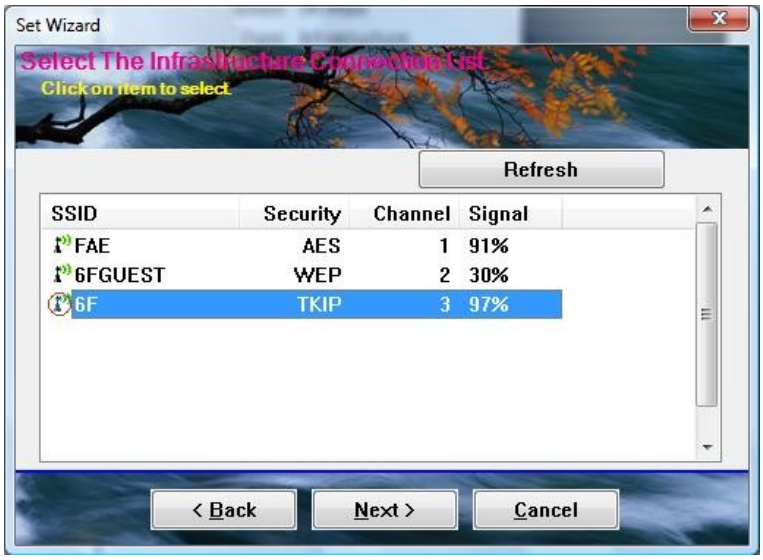
A. From the menu in the utility, select “Set Wizard”.



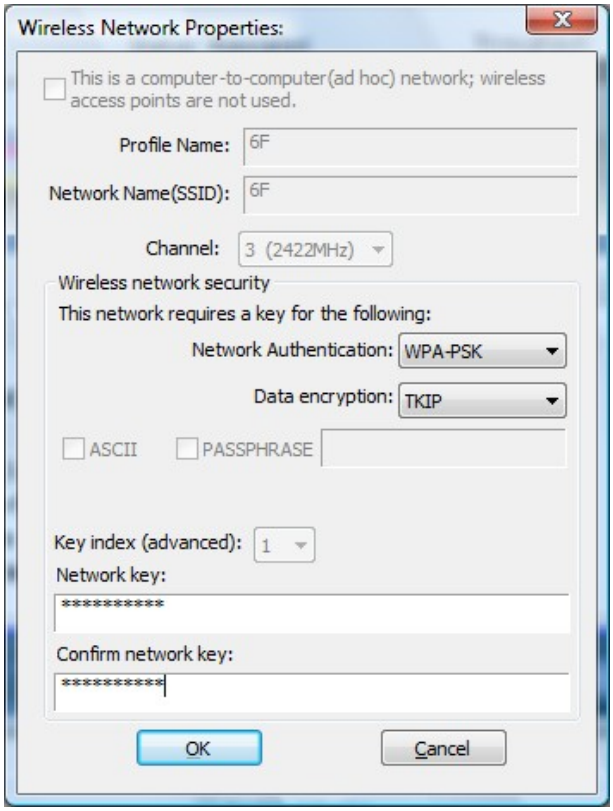
B. Select “Station (Infrastructure)” if you want to connect to the wireless network through access point or select “Station (ad hoc)” to connect to a peer-to-peer network. Click “Next”.



C. The site survey results will show up. Please select the one you'd like to connect to and click the "Next" button.

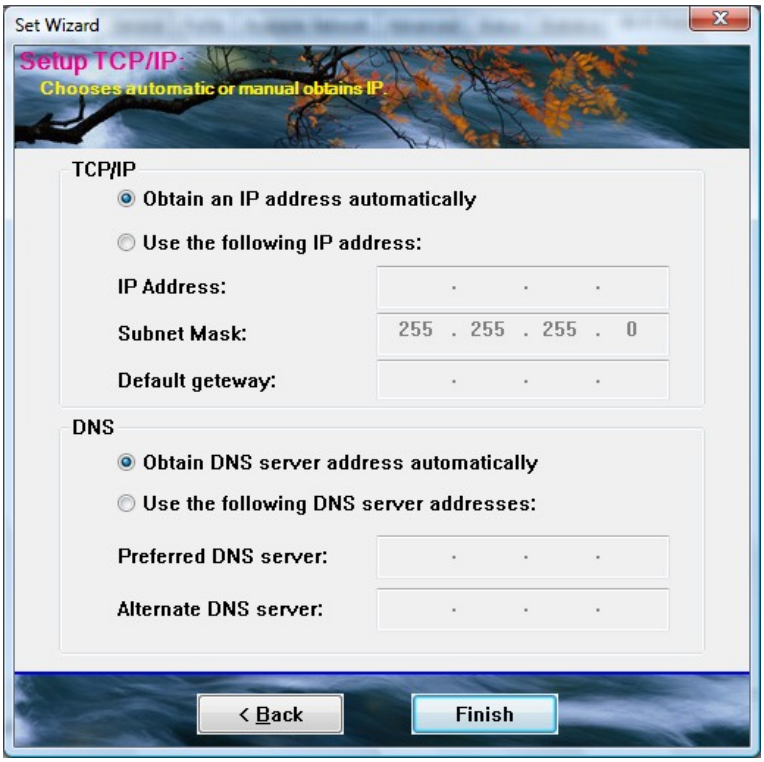


D. In the Wireless network properties dialog, please fill in the security settings for this wireless network you'd like to connect to and click "OK".

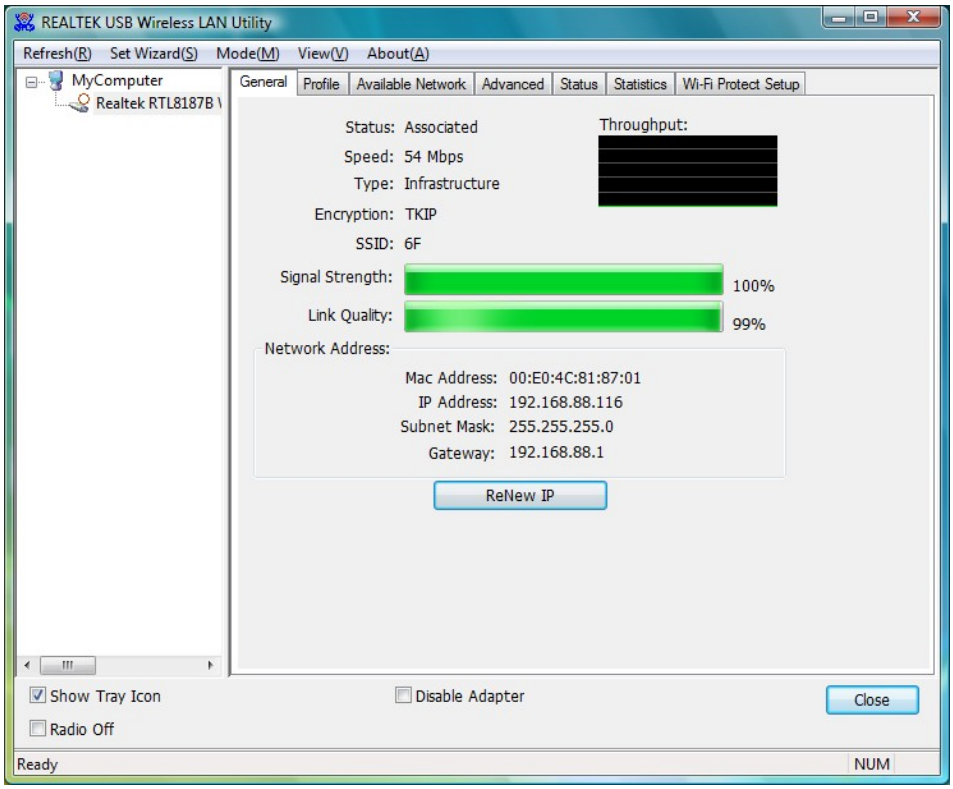


E. Please specify the IP settings for this wireless network or select to obtain the IP Address from the wireless access point directly. It is recommended to select “Obtain an IP address automatically” and “Obtain DNS server address automatically”. Please be sure that the IP Address of the adapter is in the same network segment with the wireless access point and click the “Finish” button.

For example: Assume that the wireless access point’s IP Address is 192.168.2.1 and the subnet mask is 255.255.255.0. Your computer can be configured to obtain IP Address automatically through the DHCP Server of the access point or a fixed IP Address in order to be in the same subnet as the router. The available IP Address for your computer will be 192.168.2.2 to 192.168.2.254 and the subnet mask is 255.255.255.0.



F. Now you can connect to the wireless network successfully.



4 Configuration Utility

The Configuration Utility is a powerful application that helps you configure the Wireless LAN USB Adapter and monitor the link status and the statistics during the communication process.

The Configuration Utility appears as an icon on the system tray and desktop of Windows. You can open it by double-click on the icon.

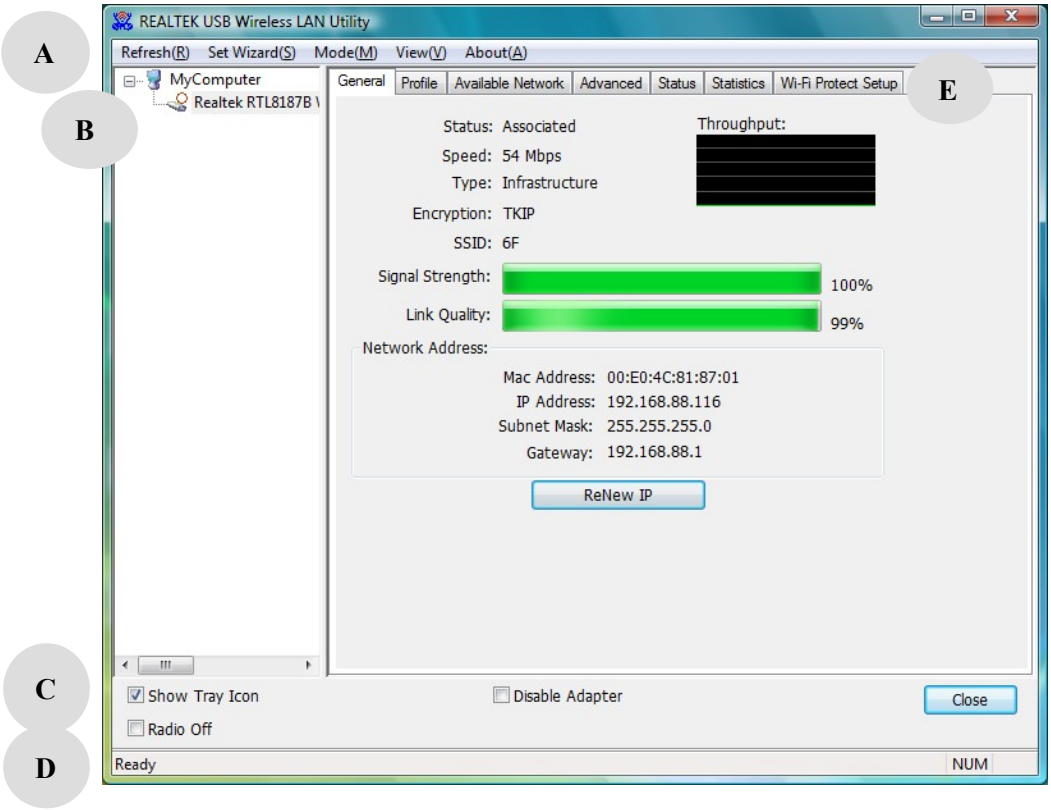
In the Desktop *In the System Tray*

Right click the icon in the system tray there are some items for you to operate the configuration utility.

- Open Config Utility
  Select “Open Config Utility” to open the configuration utility.
- Setup Wizard
  Select “SetupWizard” to open the setup wizard.
- About
  Select “About” to show the utility information.
- Hide
  Select “Hide” to hide the utility in the system tray.
- Quit
  Select “Quit” to close the utility.

3.1 Utility Overview

There are several parts in the utility screen. Please refer to the following table for the description.

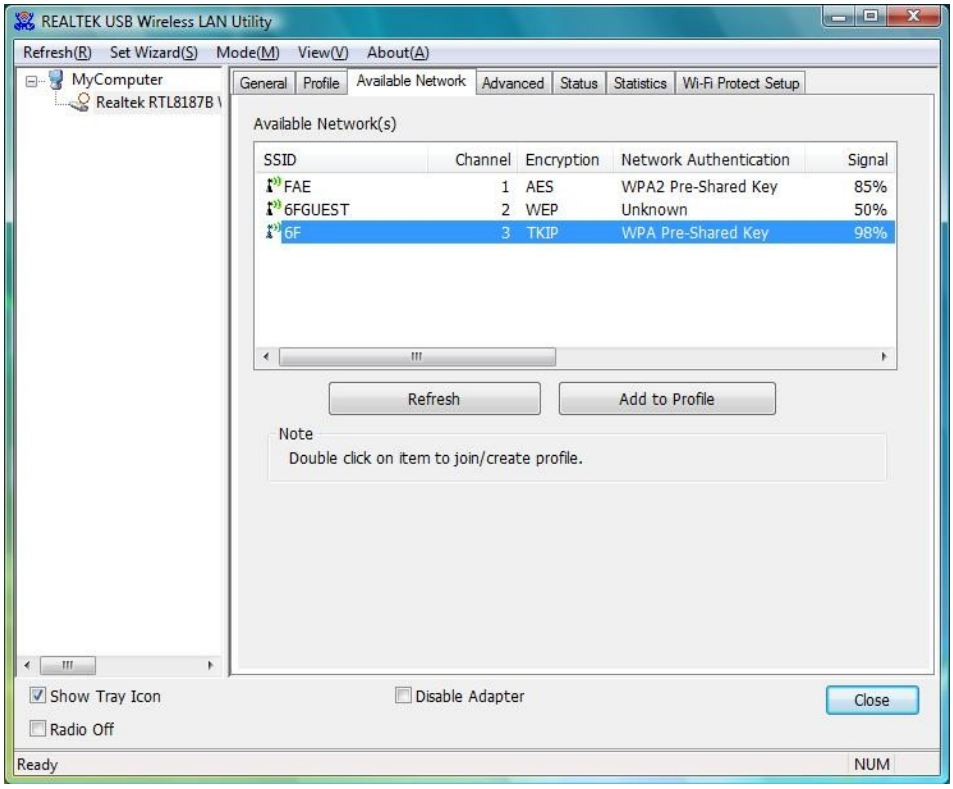


Parameter	Description
A	**Refresh** – Refresh adapter list in the “B“ block. **SetWizard** – Open the setup wizard for quick start the wireless connection. **Mode** – There are two modes: Station and Access Point. If “Station“ is selected, the adapter works as a wireless adapter. If “Access Point“ is selected, the adapter will works as a wireless AP. **View** – Enable “Status Bar“ and the “D“ block in the utility will display the current status of the utility. **About** – To check the version of the utility, select this item.
B	This is a list for you to configure several adapters in your PC from the utility.
C	**Show Tray Icon** – To show the icon in the system tray, select the item. **Radio Off** – This function is for you to turn off or turn on the radio of the adapter. If the radio is turned off, the adapter will not work. **Disable Adapter** – This function is for you to disable or enable the adapter.

Parameter	Description
D	It is the status bar that displays the current status of the utility. To close it, please disable the “Status Bar“ in the “View“ item.
E	There are several tabs in the block for you to setup the function of the adapter. Please refer to the description in the following sections.

3.2 Available Network

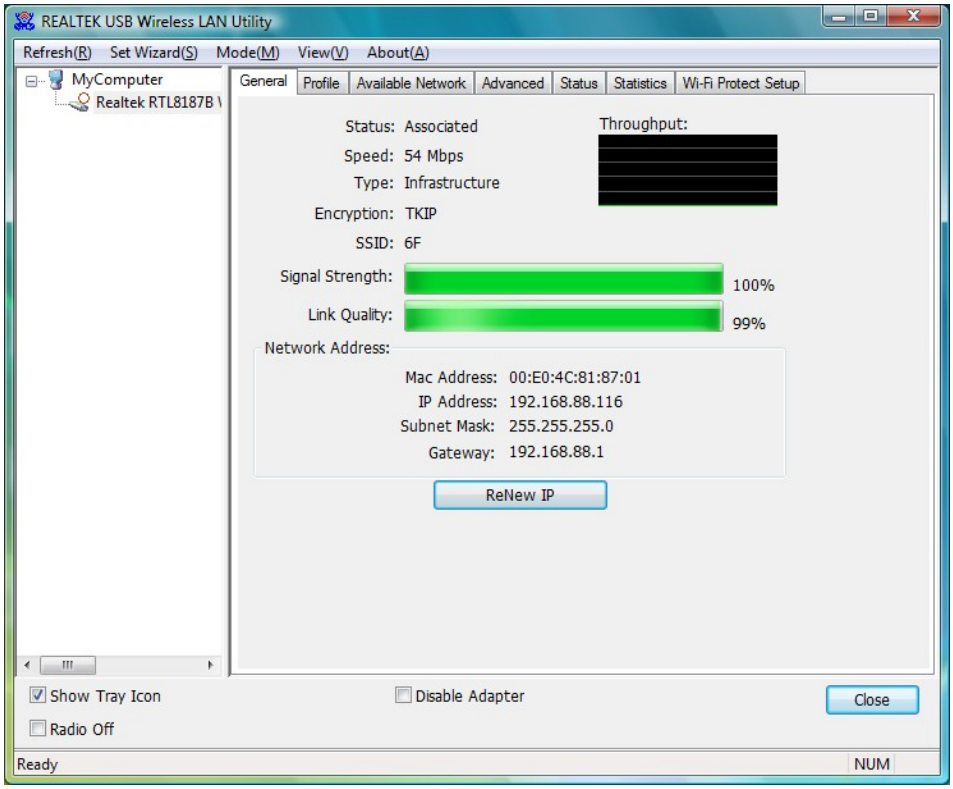
When you open the Configuration Utility, the system will scan all the channels to find all the access points/stations within the accessible range of your adapter and automatically connect to the wireless network with the highest signal strength. From the “Available Network” tab, all the networks nearby will be listed. You can change the connection to another network.



Parameter	Description
Available Network(s)	This list shows all information of the available wireless networks within the range of your adapter. The information includes SSID, Channel, Encryption, Network Authentication, Signal and etc. If you want to connect to any network on the list, double-click the selected network.
Refresh	Click “Refresh“ to update the available networks list. It is recommended that refresh the list while you have changed the connection network.
Add to Profile	A profile stores the setting of a network, so that you can connect to the network quickly. To add the selected network to a profile, click this button.

3.3 General

To check the connection status of the adapter, select “General“. This screen shows the information of Link Speed, Network Type, Encryption Method, SSID, Signal Strength, Link Quality and Network Address of the adapter.

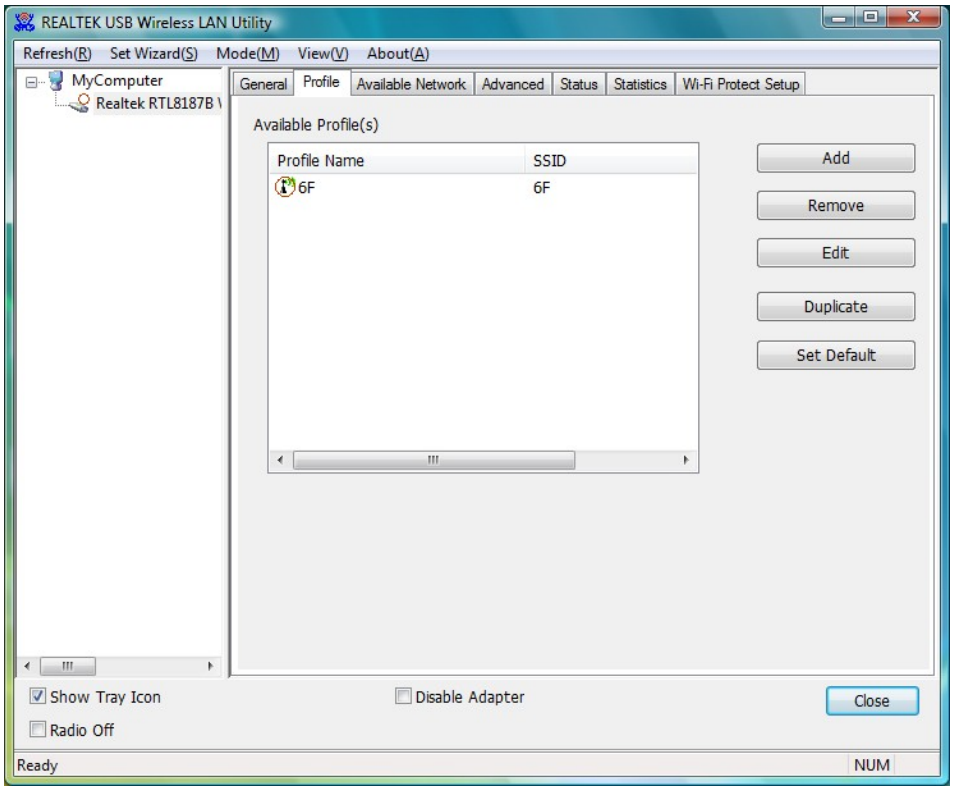


Parameter	Description
Status	It will show the connection status of the adapter.
Speed	It shows the current speed
Type	**Infrastructure** – This operation mode requires the presence of an 802.11 Access Point. All communication is done via the Access Point or Router. **IBSS** – Select this mode if you want to connect to another wireless stations in the Wireless LAN network without through an Access Point or Router.
Encryption	It displays the encryption setting of the current connection including None, WEP, TKIP or AES.
SSID	The SSID (up to 32 printable ASCII characters) is the unique name identified in a WLAN. The ID prevents the unintentional merging of two co-located WLANs.

Parameter	Description
Signal Strength	It indicates the wireless signal strength.
Link Quality	It indicates the wireless link quality.
Network Address	It shows the MAC, IP address and other information of the adapter.
Renew IP	Click this button to renew the network address settings of the adapter.

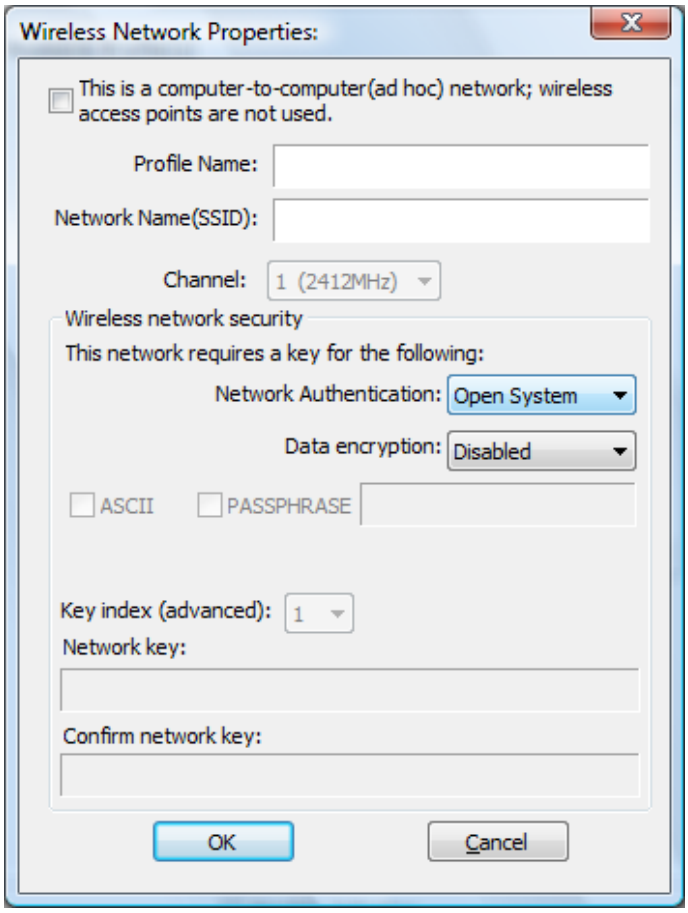
3.4 Profile

The “Profiles List” is for you to manage the networks you connect to frequently. You are able to Add/Remove/Edit/Duplicate/Set Default to manage a profile.



Parameter	Description
Available Profile(s)	This list shows the preferred networks for the wireless connection. You can add, remove, edit, duplicate the preferred networks or set one of the networks as the default connection.
Add/ Remove/ Edit Button	Click these buttons to add/ delete/ edit the selected profiles.
Duplicate	If you like to build up the new profile with the same settings as the current profile, then you can select this feature.
Set Default	To designate a profile as the default network for the connection from the available profiles list, click the button.

3.4.1 Configure the Profile



Parameter	Description
This is a computer-to-computer (ad hoc) network; wireless access points are not used.	There are two kinds of network type described as follows. **Infrastructure** – This operation mode requires the presence of an 802.11 Access Point. All communication is done via the Access Point or Router. **Ad Hoc** – Connect to another wireless adapter in the Wireless LAN network without through an Access Point or Router. If this item is selected, the adapter will work in Ad Hoc mode.
Profile Name	Define a recognizable profile name for you to identify the different networks.
Network Name (SSID)	The SSID (up to 32 printable ASCII characters) is the unique name identified in a WLAN. The ID prevents the unintentional merging of two co-located WLANs. You may specify a SSID for the adapter and then only the device with the same SSID can interconnect to the adapter.

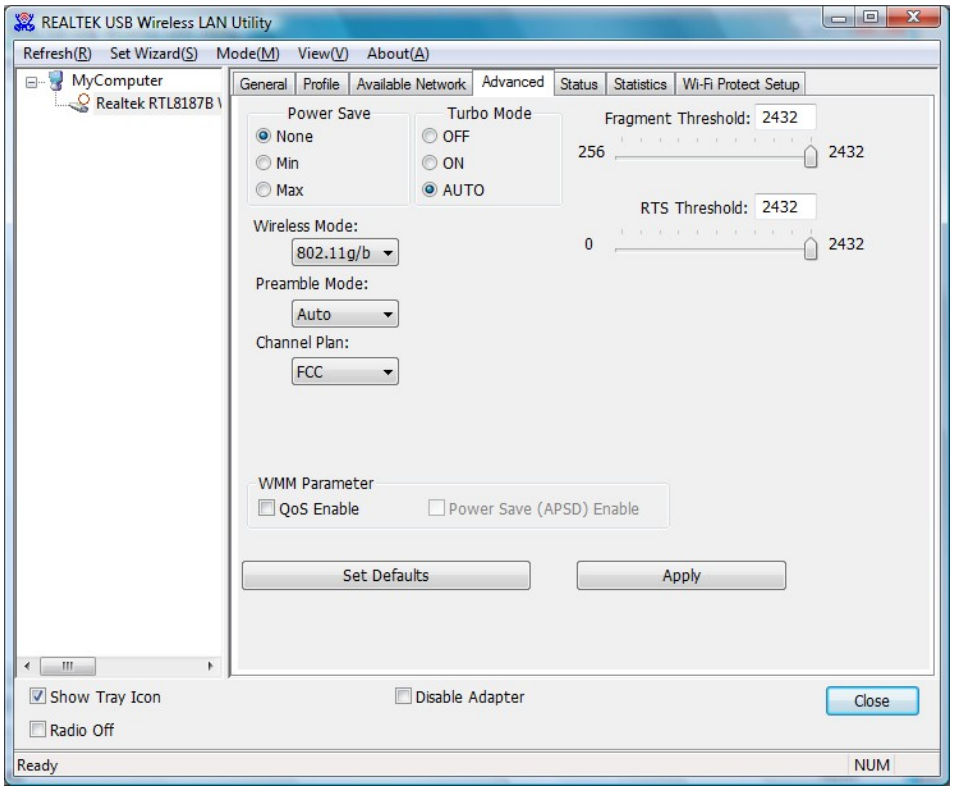
Parameter	Description
Channel	This setting is only available for Ad Hoc mode. Select the number of the radio channel used for the networking. The channel setting should be the same with the network you are connecting to.
Network Authentication	This setting has to be consistent with the wireless networks that the adapter intends to connect. Note that in Windows Vista, the adapter only supports Open System, Shared Key, WPA-PSK and WPA2-PSK security methods. **Open System** – No authentication is needed among the wireless network. **Shared Key** – Only wireless stations using a shared key (WEP Key identified) are allowed to connecting each other. **WPA-PSK** – It is a special mode designed for home and small business users who do not have access to network authentication servers. In this mode, known as Pre-Shared Key, the user manually enters the starting password in their access point or gateway, as well as in each wireless stations in the network. WPA-PSK takes over automatically from that point, keeping unauthorized users that don't have the matching password from joining the network, while encrypting the data traveling between authorized devices. **WPA2-PSK** – WPA2-PSK is also for home and small business. The difference between WPA-PSK and WPA2-PSK is that WPA2-PSK provides data encryption via the AES. In contrast, WPA-PSK uses Temporal Key Integrity Protocol (TKIP). **WPA 802.1X** – WPA provides a scheme of mutual authentication using either IEEE 802.1x/Extensible Authentication Protocol (EAP) authentication or pre-shared key (PSK) technology. It provides a high level of assurance to enterprises, small businesses and home users that data will remain protected and that only authorized users may access their networks. For enterprises that have already deployed IEEE 802.1x authentication, WPA offers the advantage of leveraging existing authentication databases and infrastructure.

	WPA2 802.1X – Like WPA, WPA2 supports IEEE 802.1x/EAP authentication or PSK technology. It also includes a new advanced encryption mechanism using the Advanced Encryption Standard (AES). AES is required to the corporate user or government users. The difference between WPA and WPA2 is that WPA2 provides data encryption via the AES. In contrast, WPA uses Temporal Key Integrity Protocol (TKIP). **WEP 802.1X** – It's a special mode for using IEEE 802.1x/EAP technology for authentication and WEP keys for data encryption.
Data Encryption	**Disabled** – Disable the WEP Data Encryption. **WEP** – Enable the WEP Data Encryption. When the item is selected, you have to continue setting the WEP Encryption keys. **TKIP** – TKIP (Temporal Key Integrity Protocol) changes the temporal key every 10,000 packets (a packet is a kind of message transmitted over a network.) This insures much greater security than the standard WEP security. **AES** – AES has been developed to ensure the highest degree of security and authenticity for digital information and it is the most advanced solution defined by IEEE 802.11i for the security in the wireless network. Note: All devices in the network should use the same encryption method to ensure the communication.
ASCII	WEP Key can be ASCII format. Alphanumeric values or signs are allowed to be the WEP key. It is more recognizable for user.
Passphrase	It is a text string with a maximum of 32 alphanumeric characters, for example: "Test". The WEP Key is based upon the Passphrase determined by you. This passphrase may not work with other vendors' products due to possible incompatibility with other vendors' passphrase generators. You must use the same passphrase or WEP key settings for all wireless computers within the network.
Key Index (advanced)	Select one of the four keys to be the data encryption key.

Parameter	Description
Network Key	The keys are used to encrypt data transmitted in the wireless network. Fill the text box by following the rules below. **64-bit** – Input 10-digit Hex values as the encryption keys. For example: “0123456aef“. **128-bit** – Input 26-digit Hex values as the encryption keys. For example: “01234567890123456789abcdef“.
Confirm Network Key	Enter the same network key to confirm.
EAP Type	**GTC** – GTC is an authentication protocol which allows the exchange of clear text authentication credentials across the network. **TLS** – TLS is the most secure of the EAP protocols but not easy to use. It requires that digital certificates be exchanged in the authentication phase. The server presents a certificate to the client. After validating the server’s certificate, the client presents a client certificate to the server for validation. **LEAP** – LEAP is a pre-EAP, Cisco-proprietary protocol, with many of the features of EAP protocols. Cisco controls the ability of other vendors to implement this protocol, so it should be selected for use only when limited vendor choice for client, access-point, and server products is not a concern. When you have set up LEAP authentication, you have to enter the user name and password of your computer. **PEAP & TTLS** – PEAP and TTLS are similar and easier than TLS in that they specify a stand-alone authentication protocol be used within an encrypted tunnel. TTLS supports any protocol within its tunnel, including CHAP, MSCHAP, MSCHAPv2 and PAP. PEAP specifies that an EAP-compliant authentication protocol must be used; this adaptor supports MD5, TLS, GTC (Generic Token Card) and MSCHAPv2. The client certificate is optional required for the authentication.
Tunnel	Includes MD5, GTC, TLS, CHAP, MSCHAP, MSCHAP-v2 and PAP.
Username	The certificate username in the RADIUS server.
Identity	User’s identity in the RADIUS server.
Password	User’s password in the RADIUS server.
Certificate	The certificate for RADIUS server for certification.

3.5 Advanced

The “Advanced” option enables you to configure more advanced settings, for example: Power Save, Turbo Mode, Wireless Mode and etc.



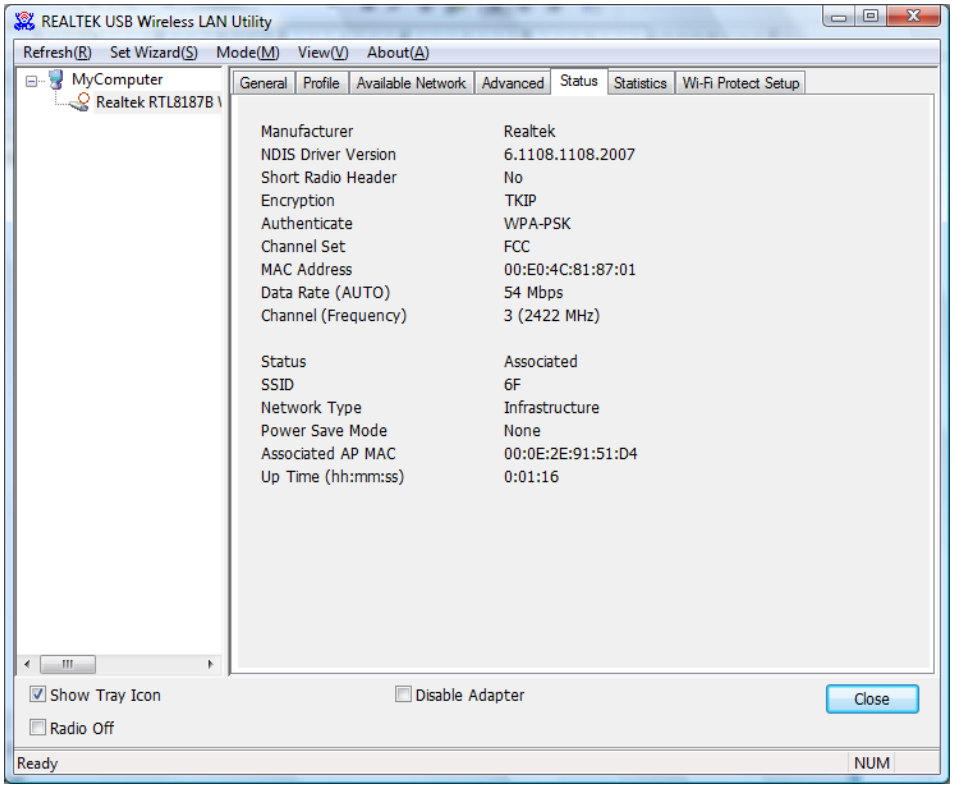
Parameter	Description
Power Save	**None** – The adapter will always set in active mode. **Min** – Enable the adapter in the power saving mode when it is idle, but some components of the adapter are still alive. In this mode, the power consumption is larger than “Max“ mode. **Max** – Enable the adapter in the power saving mode when it is idle.
Turbo Mode	**Off** – Turn off the turbo mode. **On** – Turn on the turbo mode. **Auto** – The adapter will detect the AP is RTL8186-based AP or not to transmit data in turbo mode automatically.

Parameter	Description
Wireless Mode	**802.11 b** – This adapter can be compatible with both 802.11g and 802.11b wireless stations. If there are only 802.11b wireless stations in the network, you can set the adapter to this mode. **802.11 g/b** – If you have a mix of 802.11b and 802.11g wireless stations in your network, it is recommended to setting the adapter to this mode.
Preamble Mode	The preamble defines the length of the CRC block for communication among the wireless stations. There are three mode including Long, Short and Auto. High network traffic areas should use the shorter preamble type. If “Auto“ mode is selected, the adapter will auto switch the preamble mode depending on the wireless stations that the adapter is connecting to. Note that the parameter is only active in the Ad Hoc operation mode.
Channel Plan	The available channel differs from different countries. For example: USA (FCC) is channel 1-11, Europe (ETSI) is channel 1-13. The channel of the adapter has been set depends on the country you are located. If you are in different country, you could change the channel from the pull-down list.
PSP XLink Mode	Enable this function to support PSP XLink.
WMM Parameter	**QoS Enable** – Enable this function to support WMM. **Power Save (APSD) Enable** – Enable this function to support WMM Power Save.
Fragment Threshold	The value defines the maximum size of packets; any packet size larger than the value will be fragmented. If you have decreased this value and experience high packet error rates, you can increase it again, but it will likely decrease overall network performance. Select a setting within a range of 256 to 2432 bytes. Minor change is recommended.
RTS Threshold	Minimum packet size required for an RTS (Request To Send). For packets smaller than this threshold, an RTS is not sent and the packet is transmitted directly to the wireless network. Select a setting within a range of 0 to 2432 bytes. Minor change is recommended.

Parameter	Description
Set Defaults	Let the setting values return to default.
Apply	Confirm the settings in the “Advanced“.

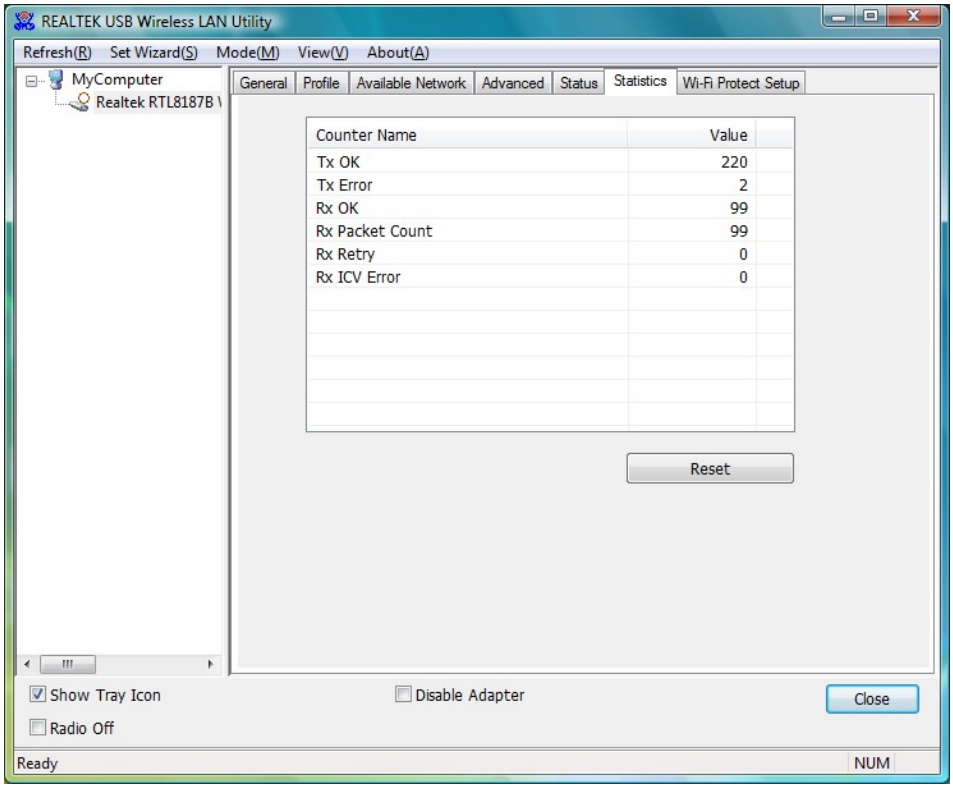
3.6 Status

This screen shows the information of manufacturer, driver version, settings of the wireless network the adapter is connecting to, linking time and link status. If you don't ensure the status of the adapter and the network you are connecting, please go to the screen for more details.



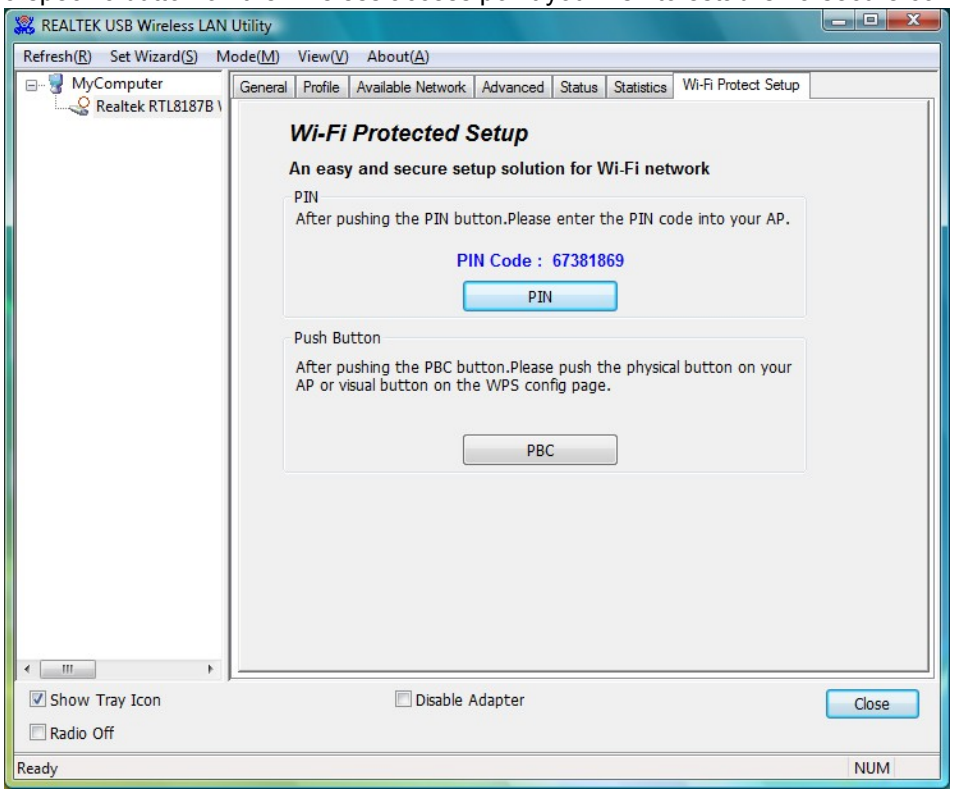
3.7 Statistics

You can get the real time information about the packet transmission and receiving status during wireless communication from the screen. If you want to recount the statistics value, please click “Reset“.



3.8 Wi-Fi Protected Setup

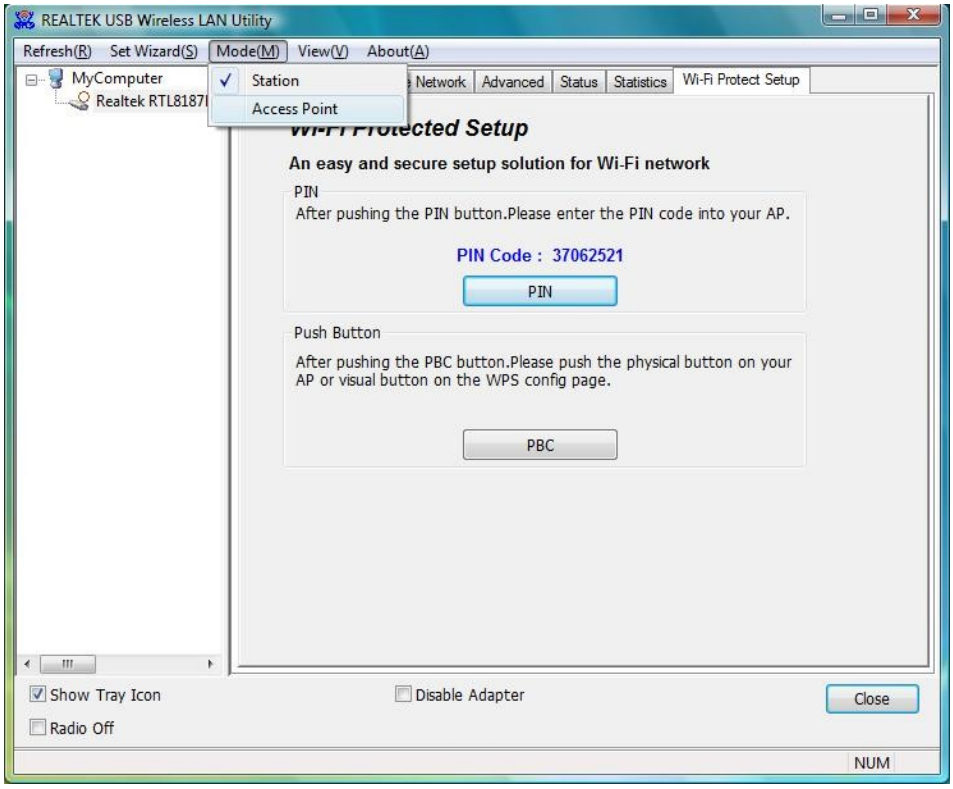
Wi-Fi Protected Setup (WPS) is the latest wireless network technology which makes wireless network setup become very simple. If you have WPS-enabled wireless access point, and you want to establish a secure connection to it, you don't have to configure the wireless access point and setup data encryption. All you have to do is go to the WPS setup page of this wireless card, click a button, and then press a specific button on the wireless access point you wish to establish a secure connection.

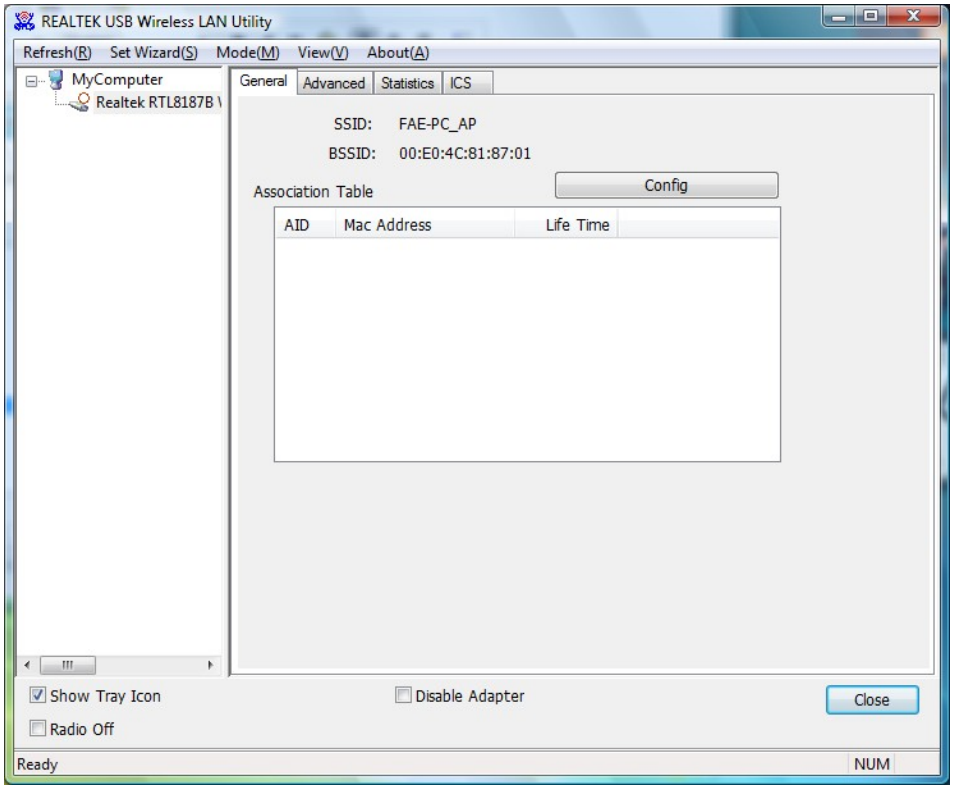

REALTEK USB Wireless LAN Utility
Refresh(R) Set Wizard(S) Mode(M) View(V) About(A)
MyComputer
Realtek RTL8187B
General Profile Available Network Advanced Status Statistics Wi-Fi Protect Setup
Wi-Fi Protected Setup
An easy and secure setup solution for Wi-Fi network
PIN
After pushing the PIN button.Please enter the PIN code into your AP.
PIN Code : 67381869
PIN
Push Button
After pushing the PBC button.Please push the physical button on your AP or visual button on the WPS config page.
PBC
Show Tray Icon
Disable Adapter
Close
Radio Off
Ready
NUM

Parameter	Description
PIN	The PIN number of your wireless network card is an eight-digit number located at the upper position of the utility. Remember it, and input the number to your wireless access point as the WPS PIN code (Please refer to the user manual of your wireless access point for instructions about how to do this). Then click 'PIN' button and wait for few seconds to one minute. If a wireless access point with correct PIN code is found, you'll be connected to that access point. Please note that you may have to click 'PIN' for few more times to try again. If you still can not connect to access point by this way, please make sure the PIN code you provided to access point is correct.
PBC	Click 'PBC' button in the utility and then start PBC pairing procedure at access point side (please refer to the instruction given by your access point's manufacturer). Please be patient (This may require several seconds to one minute to complete). Sometime WPS may fail, and you can click 'PBC' button few more times to try again.

3.9 Software AP

This adapter can run as a wireless AP. Please pull down the “Mode” menu and select “Access Point”. The relative configurations of the AP including channel, SSID, WEP encryption and so on are described as follows.

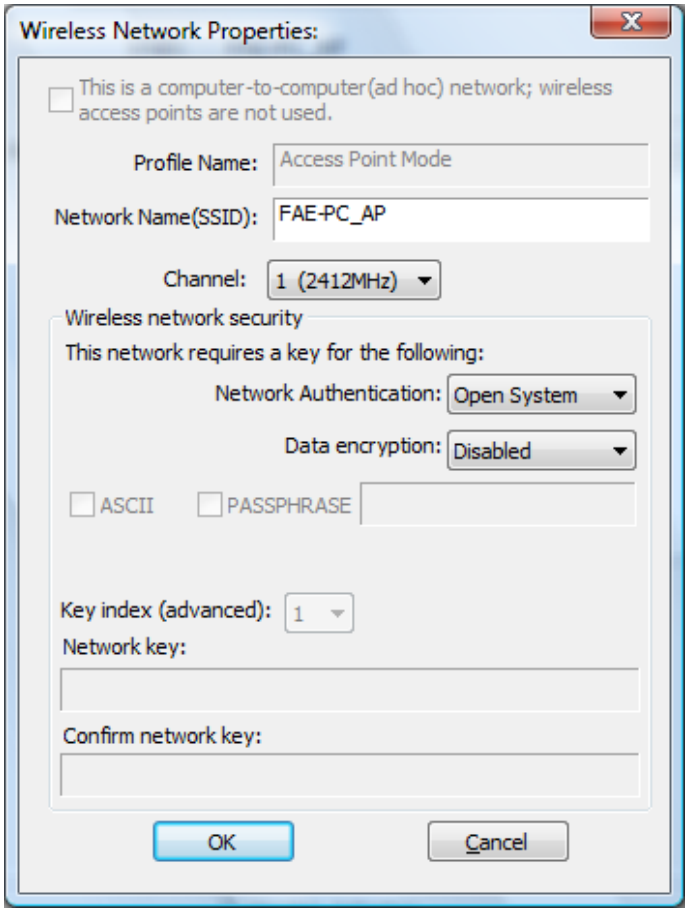




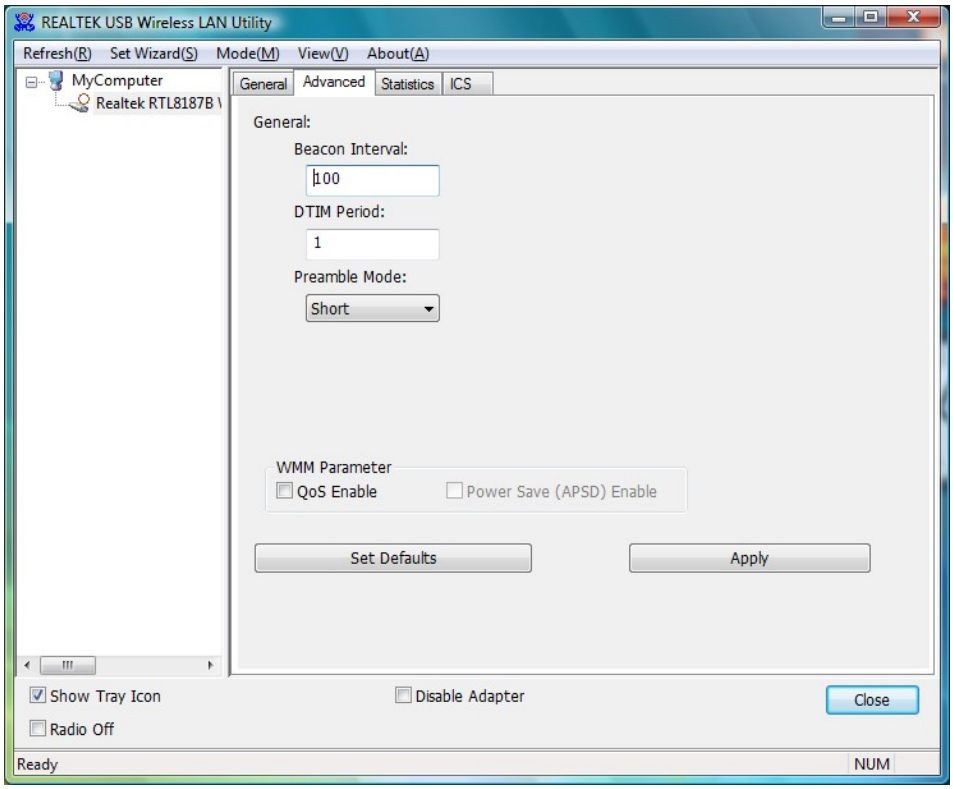
Parameter	Description
SSID	The SSID (up to 32 printable ASCII characters) is the unique name identified in a WLAN. The ID prevents the unintentional merging of two co-located WLANs. The default SSID of the AP is Full Computer Name + "_AP". Wireless adapters connect to the AP should set up the same SSID as the AP.
BSSID	Display the MAC address of the adapter.
Associate Table	All the wireless adapters connected to the software AP will be displayed in the list.
Config	Click "Config" for setting more configuration of the AP.

3.8.1 AP Properties Setting

Please refer to Section 3.4.1 for the setting of the parameters for AP. Note that Ad Hoc mode is not enabled for AP.



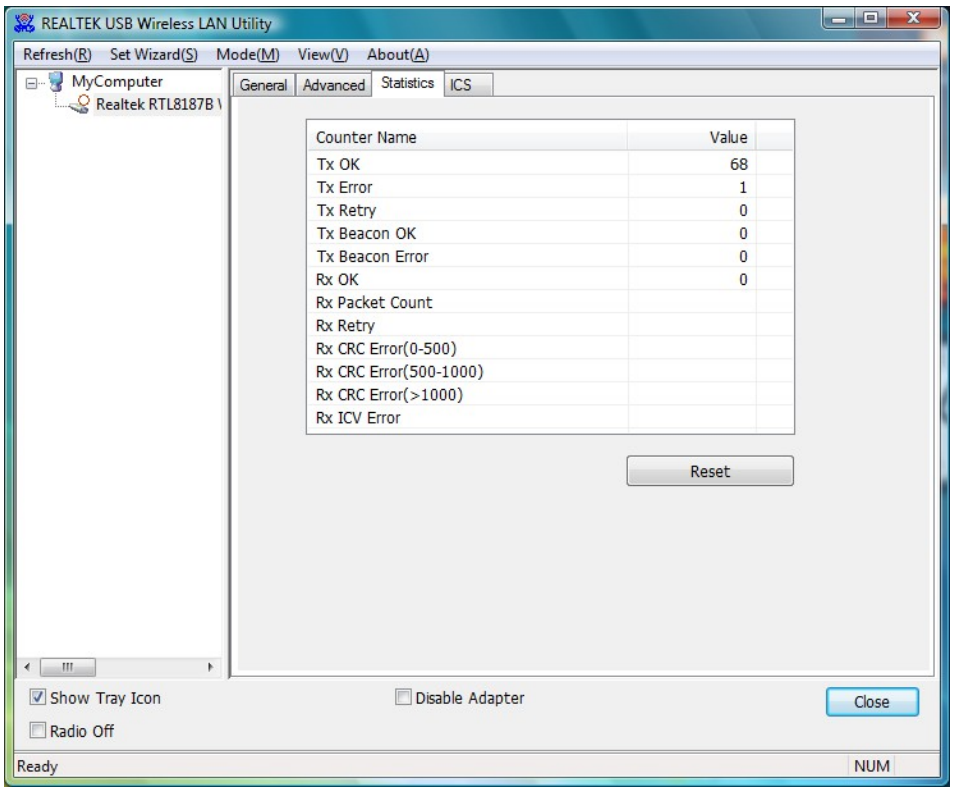
3.8.2 AP Advanced



Parameter	Description
Beacon Interval	Beacon Interval that specifies the duration between beacon packets (milliseconds). The range for the beacon period is between 20-1000 milliseconds with a typical value of 100.
DTIM Period	Determines the interval the Access Point will send its broadcast traffic. Default value is 3 beacons.
Preamble Mode	The preamble defines the length of the CRC block for communication among the wireless network. There are two mode including Long and Short. High network traffic areas should use the shorter preamble type.
WMM Parameter	**QoS Enable** – Enable this function to support WMM function. **Power Save (APSD) Enable** – Enable this function to support WMM Power Save.
Set Defaults	Set the setting values return to defaults.
Apply	Confirm the settings in the “Advanced“.

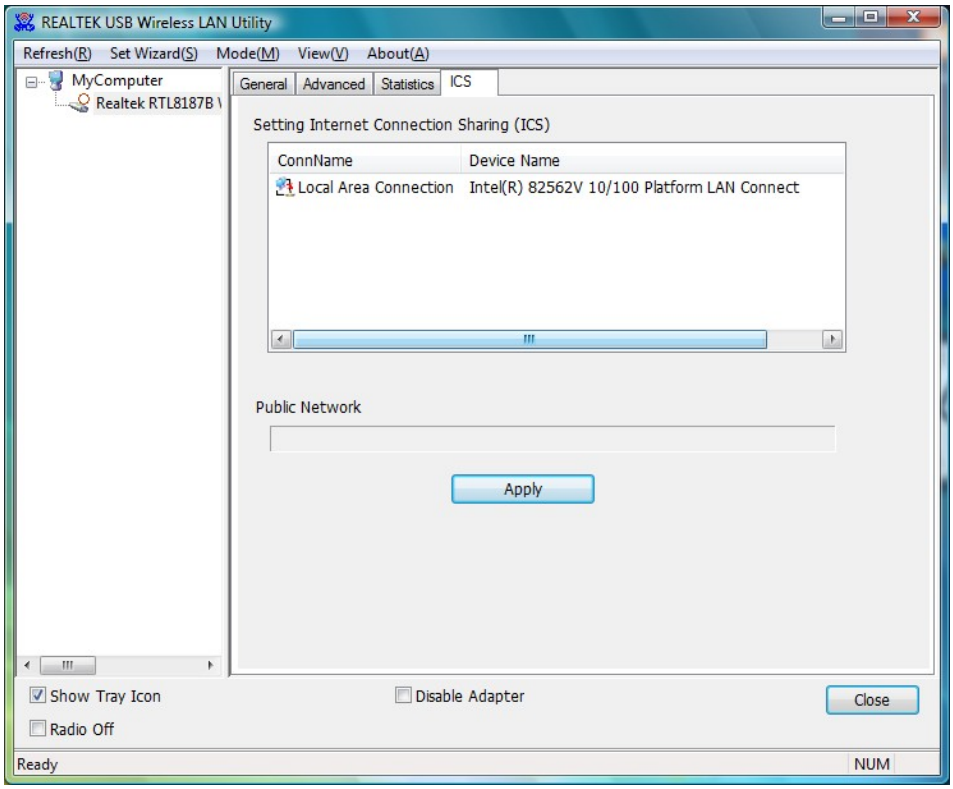
3.8.3 AP Statistics

You can get the real time information about the packet transmission and receiving status during wireless communication from the screen. If you want to recount the statistics value, please click “Reset“.



3.8.4 ICS

If you want to connect to the internet through this SoftAP, you will need to make a bridge between our SoftAP and your internet connect. Select the internet connection in your SoftAP host machine and press the “Apply” button.



5 Troubleshooting

This chapter provides solutions to problems usually encountered during the installation and operation of the adapter.

1. What is the IEEE 802.11g standard?

802.11g is the new IEEE standard for high-speed wireless LAN communications that provides for up to 54 Mbps data rate in the 2.4 GHz band. 802.11g is quickly becoming the next mainstream wireless LAN technology for the home, office and public networks.

802.11g defines the use of the same OFDM modulation technique specified in IEEE 802.11a for the 5 GHz frequency band and applies it in the same 2.4 GHz frequency band as IEEE 802.11b. The 802.11g standard requires backward compatibility with 802.11b.

The standard specifically calls for:

A. A new physical layer for the 802.11 Medium Access Control (MAC) in the 2.4 GHz frequency band, known as the extended rate PHY (ERP). The ERP adds OFDM as a mandatory new coding scheme for 6, 12 and 24 Mbps (mandatory speeds), and 18, 36, 48 and 54 Mbps (optional speeds). The ERP includes the modulation schemes found in 802.11b including CCK for 11 and 5.5 Mbps and Barker code modulation for 2 and 1 Mbps.

B. A protection mechanism called RTS/CTS that governs how 802.11g devices and 802.11b devices interoperate.

2. **What is the IEEE 802.11b standard**？

The IEEE 802.11b Wireless LAN standard subcommittee, which formulates the standard for the industry. The objective is to enable wireless LAN hardware from different manufactures to communicate.

3. **What does IEEE 802.11 feature support**？

The product supports the following IEEE 802.11 functions:

- CSMA/CA plus Acknowledge Protocol
- Multi-Channel Roaming
- Automatic Rate Selection
- RTS/CTS Feature
- Fragmentation
- Power Management

4. **What is Ad-hoc**？

An Ad-hoc integrated wireless LAN is a group of computers, each has a Wireless LAN adapter, Connected as an independent wireless LAN. Ad hoc wireless LAN is applicable at a departmental scale for a branch or SOHO operation.

5. **What is Infrastructure**？

An integrated wireless and wireless and wired LAN is called an Infrastructure configuration. Infrastructure is applicable to enterprise scale for wireless access to central database, or wireless application for mobile workers.

6. **What is BSS ID？**

A specific Ad hoc LAN is called a Basic Service Set (BSS). Computers in a BSS must be configured with the same BSS ID.

7. **What is WEP？**

WEP is Wired Equivalent Privacy, a data privacy mechanism based on a 40 bit shared key algorithm, as described in the IEEE 802 .11 standard.

8. What is TKIP?

TKIP is a quick-fix method to quickly overcome the inherent weaknesses in WEP security, especially the reuse of encryption keys. TKIP is involved in the IEEE 802.11i WLAN security standard, and the specification might be officially released by early 2003.

9. What is AES?

AES (Advanced Encryption Standard), a chip-based security, has been developed to ensure the highest degree of security and authenticity for digital information, wherever and however communicated or stored, while making more efficient use of hardware and/or software than previous encryption standards. It is also included in IEEE 802.11i standard. Compare with AES, TKIP is a temporary protocol for replacing WEP security until manufacturers implement AES at the hardware level.

10. **Can Wireless products support printer sharing？**

Wireless products perform the same function as LAN products. Therefore, Wireless products can work with Netware, Windows 2000, or other LAN operating systems to support printer or file sharing.

11. **Would the information be intercepted while transmitting on air？**

WLAN features two-fold protection in security. On the hardware side, as with Direct Sequence Spread Spectrum technology, it has the inherent security feature of scrambling. On the software side, WLAN series offer the encryption function (WEP) to enhance security and Access Control. Users can set it up depending upon their needs.

12. **What is DSSS？What is FHSS？And what are their differences？**

Frequency-hopping spread-spectrum (FHSS) uses a narrowband carrier that changes frequency in a pattern that is known to both transmitter and receiver. Properly synchronized, the net effect is to maintain a single logical channel. To an unintended receiver, FHSS appears to be short-duration impulse noise. Direct-sequence spread-spectrum (DSSS) generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code). The longer the chip is, the greater the probability that the original data can be recovered. Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without-the need for retransmission. To an unintended receiver, DSSS appears as low power wideband noise and is rejected (ignored) by most narrowband receivers.

13. **What is Spread Spectrum**？

Spread Spectrum technology is a wideband radio frequency technique developed by the military for use in reliable, secure, mission-critical communication systems. It is designed to trade off bandwidth efficiency for reliability, integrity, and security. In other words, more bandwidth is consumed than in the case of narrowband transmission, but the trade off produces a signal that is, in effect, louder and thus easier to detect, provided that the receiver knows the parameters of the spread-spectrum signal being broadcast. If a receiver is not tuned to the right frequency, a spread –spectrum signal looks like background noise. There are two main alternatives, Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS).